

DATA ITEM DESCRIPTION	
<b>1. TITLE</b> Configuration Management Documentation	<b>2. NUMBER</b> F001
<b>3. DESCRIPTION/PURPOSE</b> <p>The Configuration Management Documentation shall present the contractor's approach to maintaining configuration control over the system during design, development, testing, and deployment, including all hardware, software, firmware, and telecommunications equipment.</p>	
<b>4. DATA REQUIREMENTS</b> <p><b>Reference:</b> SOW paragraph 4.1.2, ISO/IEC 15408-3, ACM_CAP.3, ACM_SCP.1, ACM_AUT.1</p> <p><b>Contents:</b>  The CM system shall uniquely identify all configuration items.</p> <p>The CM system shall provide measures such that only authorized changes are made to the configuration items.</p> <p>The CM documentation shall include a configuration list and a CM plan.</p> <p>The CM documentation shall describe the method used to uniquely identify the configuration items.</p> <p>The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.</p> <p>The configuration list shall describe the configuration items that comprise the TOE.</p> <p>The reference for the TOE shall be unique to each version of the TOE.</p> <p>The TOE shall be labeled with its reference.</p> <p>The CM plan shall describe how the CM system is used.</p> <p>The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.</p> <p>The CM documentation shall show that the CM system, at a minimum, tracks the following: (a) the TOE implementation representation, (b) design documentation, (c) test documentation, (d) user documentation, (e) administrator documentation, and (f) CM documentation.</p> <p>The CM documentation shall describe how configuration items are tracked by the CM system.</p> <p>The CM system shall provide an automated means by which only authorized changes are made to the TOE implementation representation.</p> <p>The CM system shall provide an automated means to support the generation of the TOE.</p> <p>The CM Plan shall describe the automated tools used in the CM system.</p> <p>The CM plan shall describe how the automated tools are used in the CM system.</p>	

DATA ITEM DESCRIPTION	
<b>1. TITLE</b> Delivery Procedures	<b>2. NUMBER</b> F002
<b>3. DESCRIPTION/PURPOSE</b> <p>The requirements for delivery call for system control and distribution facilities and procedures that provide assurance that the recipient receives the TOE that the sender intended to send, without any modifications. For a valid delivery, what is received must correspond precisely to the TOE master copy, thus avoiding any tampering with the actual version, or substitution of a false version. The Delivery Procedures address these concerns.</p>	
<b>4. DATA REQUIREMENTS</b> <p><b>Reference:</b> SOW paragraph 4.1.2, ISO/IEC 15408-3, ADO_DEL.1</p> <p><b><u>Contents:</u></b></p> <p>The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site(s).</p>	

DATA ITEM DESCRIPTION	
<b>1. TITLE</b> Installation, Generation, and Start-up Procedures	<b>2. NUMBER</b> F003
<b>3. DESCRIPTION/PURPOSE</b> Installation, generation, and start-up procedures are useful for ensuring that the TOE has been installed, generated, and started up in a secure manner as intended by the developer. The requirements for installation, generation and start-up call for a security transition from the TOE's implementation representation being under configuration control to its initial operation in the user environment.	
<b>4. DATA REQUIREMENTS</b> <b>Reference:</b> SOW paragraph 4.1.2, ISO/IEC 15408-3, ADO_IGS.1 <b><u>Contents:</u></b> The documentation shall describe all the steps necessary for secure installation, generation, and start-up of the TOE.	

DATA ITEM DESCRIPTION	
<b>1. TITLE</b> Functional Specification	<b>2. NUMBER</b> F004
<b>3. DESCRIPTION/PURPOSE</b> <p>The functional specification is a high-level description of the user-visible interface and behavior of the TOE security functions. It is an instantiation of the TOE security functional requirements. The functional specification has to show that all TOE security functional requirements are addressed.</p>	
<b>4. DATA REQUIREMENTS</b> <p><b>Reference:</b> SOW paragraph 4.1.2, ISO/IEC 15408-3, ADV_FSP.1</p> <p><b>Contents:</b></p> <p>The functional specification shall describe the TOE security function (TSF) and its external interfaces using an informal style.</p> <p>The functional specification shall be internally consistent.</p> <p>The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions, and error messages, as appropriate.</p> <p>The functional specification shall completely represent the TOE security policy.</p>	

DATA ITEM DESCRIPTION	
<b>1. TITLE</b> High-level Design Documentation	<b>2. NUMBER</b> F005
<b>3. DESCRIPTION/PURPOSE</b>  <p>The high-level design of a TOE provides a description of the TOE security functions in terms of major structural units (i.e. subsystems) and relates these units to the functions that they provide. The high-level design requirements are intended to provide assurance that the Toe provides an architecture appropriate to implement the TOE security functional requirements.</p> <p>The high-level design refines the functional specification (DID F004) into subsystems. For each subsystem of the TOE security functions, the high-level design describes its purpose and function, and identifies the security functions contained in the subsystem. The interrelationships of all subsystems are also defined in the high-level design. These interrelationships will be represented as external interfaces for data flow, control flow, etc., as appropriate.</p>	
<b>4. DATA REQUIREMENTS</b> <p><b>Reference:</b> SOW paragraph 4.1.2, ISO/IEC 15408-3, ADV_HDL.2</p> <p><b>Contents:</b>  The presentation of the high-level design shall be informal.</p> <p>The high-level design shall be internally consistent.</p> <p>The high-level design shall describe the structure of the TOE security Function (TSF) in terms of subsystems.</p> <p>The high-level design shall describe the security functionality provided by each subsystem of the TSF.</p> <p>The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, software, or firmware.</p> <p>The high-level design shall identify all interfaces to the subsystems of the TSF.</p> <p>The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.</p> <p>The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.</p> <p>The high-level design shall describe the separation of the TOE into TOE security policy enforcing and other subsystems.</p> <p>The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TOE security function, providing details of effects, exceptions, and error messages, as appropriate.</p> <p>The high-level design shall describe the separation of the TOE into security policy enforcing and other subsystems.</p>	

DATA ITEM DESCRIPTION	
<b>1. TITLE</b> Requirements Correspondence Report	<b>2. NUMBER</b> F006
<b>3. DESCRIPTION/PURPOSE</b> <p>The correspondence between the various TOE security function representations (i.e. Security Target DID F019, Functional Specification DID F004, and High-level Design DID F005) addresses the correct and complete instantiation of the requirements to the last abstract TOE security function representation provided. This conclusion is achieved by step-wise refinement and the cumulative results of correspondence determinations between all adjacent abstractions of representation.</p>	
<b>4. DATA REQUIREMENTS</b> <p><b>Reference:</b> SOW paragraph 4.1.2, ISO/IEC 15408-3, ADV_RCR.1</p> <p><b><u>Contents:</u></b></p> <p>For each adjacent pair of provided TOE security function (TSF) representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF is correctly and completely refined in the less abstract TSF representation.</p>	

DATA ITEM DESCRIPTION	
<b>1. TITLE</b>	<b>2. NUMBER</b>
Security Policy Model Documentation	F007
<b>3. DESCRIPTION/PURPOSE</b>  <p>The purpose of the Security Policy Model documentation is to provide additional assurance that the security functions in the functional specification (DID F004) enforce the policies in the TOE security policy. This is accomplished via the development of a security policy model that is based on a subset of the policies of the TOE security policy, and establishing a correspondence between the functional specification, the security policy model, and these policies of the TOE security policy.</p>	
<b>4. DATA REQUIREMENTS</b>  <p><b>Reference:</b> SOW paragraph 4.1.2, ISO/IEC 15408-3, ADV_SPM.1</p> <p><b><u>Contents:</u></b></p> <p>The TOE security policy model shall be informal.</p> <p>The TOE security policy model shall describe the rules and characteristics of all policies that can be modeled.</p> <p>The TOE security policy model shall include a rationale that demonstrates that it is consistent and complete with respect to all policies that can be modeled.</p> <p>The demonstration of correspondence between the TOE security policy model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the TOE security policy model.</p>	

DATA ITEM DESCRIPTION	
<b>1. TITLE</b> Administrator Guidance Documentation	<b>2. NUMBER</b> F008
<b>3. DESCRIPTION/PURPOSE</b> <p>The Administrator Guidance Documentation shall present all the information needed by a system administrator in order to operate the system in a known secure state at all times.</p>	
<b>4. DATA REQUIREMENTS</b> <p><b>Reference:</b> SOW paragraph 4.1.2, ISO/IEC 15408-3, AGD_ADM.1</p> <p><b>Contents:</b></p> <p>The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.</p> <p>The administrator guidance shall describe how to administer the TOE in a secure manner.</p> <p>The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.</p> <p>The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.</p> <p>The administrator guidance shall describe all security parameters under the control of the administrator indicating secure values as appropriate.</p> <p>The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TOE security function.</p> <p>The administrator guidance shall be consistent with all other documentation supplied for evaluation.</p> <p>The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.</p>	

DATA ITEM DESCRIPTION	
<b>1. TITLE</b> User Guidance Documentation	<b>2. NUMBER</b> F009
<b>3. DESCRIPTION/PURPOSE</b> <p>The User Guidance Documentation shall present all the information needed by an end-user in order to operate the system in a known secure state at all times.</p>	
<b>4. DATA REQUIREMENTS</b> <p><b>Reference:</b> SOW paragraph 4. 1.2, ISO/IEC 15408-3, AGD_USR.1</p> <p><b>Contents:</b></p> <p>The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.</p> <p>The user guidance shall describe the use of user-accessible security functions provided by the TOE.</p> <p>The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.</p> <p>The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the TOE security environment described in Section 3 of the Protection Profile.</p> <p>The user guidance shall be consistent with all other documentation supplied for evaluation.</p> <p>The user guidance shall describe all security requirements for the IT environment that are relevant to the user.</p>	

DAT A ITEM DESCRIPTION	
<b>1. TITLE</b> Development Security Documentation	<b>2. NUMBER</b> F023
<b>3. DESCRIPTION/PURPOSE</b> <p>Development security is concerned with physical, procedural, personnel, and other security measures that may be used in the development environment to protect the TOE. It includes the physical security of the development location and any procedures used to select development staff.</p>	
<b>4. DATA REQUIREMENTS</b> <p><b>Reference:</b> SOW paragraph 4.1.2, ISO/IEC 15408-3, ADV_DVS.1</p> <p><b><u>Contents:</u></b></p> <p>The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.</p> <p>The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.</p>	

DATA ITEM DESCRIPTION	
<b>1. TITLE</b> Flaw Remediation Procedures	<b>2. NUMBER</b> F024
<b>3. DESCRIPTION/PURPOSE</b> <p>Flaw remediation requires that discovered security flaws be tracked and corrected by the developer. Although future compliance with flaw remediation procedures cannot be determined at the time of the TOE evaluation, it is possible to evaluate the policies and procedures that a developer has in place to track and correct flaws, and to distribute the flaw information and corrections.</p>	
<b>4. DATA REQUIREMENTS</b> <p><b>Reference:</b> SOW paragraph 4.1.2, ISO/IEC 15408-3, ALC_FLR.2</p> <p><b><u>Contents:</u></b></p> <p><b>The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.</b></p> <p><b>The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.</b></p> <p>The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.</p> <p>The flaw remediation procedures documentation shall describe the methods used to provide flow information, corrections and guidance on corrective actions to TOE users.</p> <p>The procedures for processing reported security flaws shall ensure that any reported flaws are corrected and the correction issued to TOE users.</p> <p>The procedures for processing reported security flaws shall provide safeguards that any correction to these security flaws do not introduce any new flaws.</p>	

DATA ITEM DESCRIPTION	
<b>1. TITLE</b> Test Coverage Documentation	<b>2. NUMBER</b> F0010
<b>3. DESCRIPTION/PURPOSE</b>  The purpose of the test coverage documentation is to ensure the completeness of the text coverage; in particular it addresses the extent to which the security functions are tested and whether or not the testing is sufficiently extensive to demonstrates that the security functions operate as specified.	
<b>4. DATA REQUIREMENTS</b>  <b>Reference:</b> SOW paragraph 4.1.2, ISO/IEC 15408-3, ATE_COV.2  <b>Contents:</b>  The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TOE security function as described in the functional specification.  The analysis of the test coverage shall demonstrate that the correspondence between the TOE security as described in the functional specification and the tests identified in the test documentation is complete.	

DATA ITEM DESCRIPTION	
<b>1. TITLE</b> Test Depth Documentation	<b>2. NUMBER</b> F020
<b>3. DESCRIPTION/PURPOSE</b> <p>The subsystems of a TSF provide a high-level description of the internal workings of the TSF. Testing at the level of the subsystems, in order to demonstrate the presence of any flaws, provides assurance that the TSF subsystems have been correctly realized. The Test Depth Documentation captures this evidence.</p>	
<b>4. DATA REQUIREMENTS</b> <p><b>Reference:</b> SOW paragraph 4.1.2, ISO/IEC 15408-3, ATE_DPT.1</p> <p><b><u>Contents:</u></b></p> <p>The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TOE security function operates in accordance with the high-level design.</p>	

DATA ITEM DESCRIPTION	
<b>1. TITLE</b> Functional Testing Documentation	<b>2. NUMBER</b> F011
<b>3. DESCRIPTION/PURPOSE</b> <p>The purpose of the functional testing documentation is to establish that the functional testing performed by the developer demonstrates that the security functions exhibit the properties necessary to satisfy the functional requirements of the Protection Profile and Security Target. Such functional testing provides assurance that the security functions satisfy at least the security functional requirements. Functional tests are focused on the type and amount of documentation or support tools required and what is to be demonstrated through developer testing. Functional testing is not limited to positive confirmation that the required security functions are provided, but may also include negative testing to check for the absence of particular undesired behavior (often based on the inversion of functional requirements).</p>	
<b>4. DATA REQUIREMENTS</b> <p><b>Reference:</b> SOW paragraph 4.1.2, ISO/IEC 15408-3, ATE_FUN.1</p> <p><b>Contents:</b></p> <p>The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.</p> <p>The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.</p> <p>The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies of the results of other tests.</p> <p>The expected test results shall show the anticipated outputs from a successful execution of the tests.</p> <p>The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.</p>	

DATA ITEM DESCRIPTION	
<b>1. TITLE</b> Independent Testing Documentation	<b>2. NUMBER</b> F012
<b>3. DESCRIPTION/PURPOSE</b> <p>The purpose of the independent testing documentation is to demonstrate that the security functions perform as specified. In addition, the intent is to counter the risk of an incorrect assessment of the test outcomes on the part of the developer that results in the incorrect implementation of the specifications, or overlooks code that is non-compliant with the specifications.</p>	
<b>4. DATA REQUIREMENTS</b> <p><b>Reference:</b> SOW paragraph 4.1.2, ISO/IEC 15408-3, ATE_IND.2.1</p> <p><b><u>Contents:</u></b></p> <p>The TOE shall be suitable for testing.</p> <p>The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TOE security function.</p>	

DATA ITEM DESCRIPTION	
<b>1. TITLE</b> Covert Channel Analysis Documentation	<b>2. NUMBER</b> F022
<b>3. DESCRIPTION/PURPOSE</b> <p>Covert channel analysis is carried out to determine the existence and potential capacity of unintended signally channels (i.e. illicit information flows) that may be exploited. The assurance requirement address the threat that unintended and exploitable signally paths exist that may be exercised to violate the SFP. The objective of this documentation is to identify covert channels that are identifiable through an informal search for covert channels.</p>	
<b>4. DATA REQUIREMENTS</b> <p><b>Reference:</b> SOW paragraph 4.1.2, ISO/IEC 15408-3, AVA_CCA.1</p> <p><b><u>Contents:</u></b></p> <p>The analysis documentation shall identify covert channels and estimate their capacity.</p> <p>The analysis documentation shall describe the procedures used for determining the existence of covert channels and the information needed to carry out the covert channel analysis.</p> <p>The analysis documentation shall describe all assumptions made during the covert channel analysis.</p> <p>The analysis documentation shall describe the method used for estimating channel capacity, based on worst-case scenarios.</p> <p>The analysis documentation shall describe the worst-case exploitation scenario for each identified covert channel.</p>	

DATA ITEM DESCRIPTION	
<b>1. TITLE</b> Misuse Analysis Documentation	<b>2. NUMBER</b> F021
<b>3. DESCRIPTION/PURPOSE</b> <p>The purpose of this analysis is to ensure that misleading, unreasonable and conflicting guidance is absent from the guidance documentation, and that secure procedures for all modes of operation have been addressed. Insecure states should be easy to detect.</p>	
<b>4. DATA REQUIREMENTS</b> <p><b>Reference:</b> SOW paragraph 4.1.2, ISO/IEC 15408-3, AVA_MSU.1</p> <p><b><u>Contents:</u></b></p> <p><b>The guidance documentation shall identify all possible modes of operation of the TOE including operation following failure or operational error, their consequences and implications for maintaining secure operation.</b></p> <p><b>The guidance documentation shall be complete, clear, consistent, and reasonable.</b></p> <p><b>The guidance documentation shall list all assumptions about the intended environment.</b></p> <p><b>The guidance documentation shall list all requirements for external security measures, including external procedural, physical and personnel controls.</b></p>	

DATA ITEM DESCRIPTION	
<b>1. TITLE</b> Strength of Function Documentation	<b>2. NUMBER</b> F013
<b>3. DESCRIPTION/PURPOSE</b>  <p>Even if a TOE security function cannot be bypassed, deactivated, or corrupted, it may still be possible to defeat it because there is a vulnerability in the concept of its underlying security mechanisms. For those functions a qualification of their security behavior can be made using the results of a quantitative or statistical analysis of the security behavior of these mechanisms and the effort required to overcome them. The qualification is made in the form of a strength of TOE security function claim.</p>	
<b>4. DATA REQUIREMENTS</b>  <p><b>Reference:</b> SOW paragraph 4.1.2, ISO/IEC 15408-3, AVA_SOF.1</p> <p><b><u>Contents:</u></b></p> <p>For each mechanism with a strength of TOE security function claim, the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the Protection Profile and Security Target.</p> <p>For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the Protection Profile and Security Target.</p> <p>The documentation shall show, for all identified vulnerabilities that the vulnerability cannot be exploited in the intended environment for the TOE.</p>	

DATA ITEM DESCRIPTION	
<b>1. TITLE</b> Vulnerability Analysis Documentation	<b>2. NUMBER</b> F014
<b>3. DESCRIPTION/PURPOSE</b> A vulnerability analysis is performed by the developer to ascertain the presence of obvious security vulnerabilities, and to confirm that they cannot be exploited in the intended environment for the TOE.	
<b>4. DATA REQUIREMENTS</b> <b>Reference:</b> SOW paragraph 4.1.2, ISO/IEC 15408-3, AVA_VLA.1 <b><u>Contents:</u></b> The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.	

DATA ITEM DESCRIPTION	
<b>1. TITLE</b> Assurance Maintenance Plan	<b>2. NUMBER</b> F0015
<b>3. DESCRIPTION/PURPOSE</b> <p>The Assurance Maintenance Plan identifies the plans and procedures a developer must implement in order to ensure that the assurance that was established in the certified TOE is maintained as changes are made to the TOE or its environment. The Assurance Maintenance Plan is specific to the TOE, and is tailored to the developer's own practices and procedures.</p>	
<b>4. DATA REQUIREMENTS</b> <p><b>Reference:</b> SOW paragraph 4.1.2, ISO/IEC 15408-3, AMA_AMP.1</p> <p><b>Contents:</b>  <b>The Assurance Maintenance (AM) Plan shall contain or reference a brief description of the TOE, including the security functionality it provides.</b></p> <p><b>The AM Plan shall identify the certified version of the TOE, and shall reference the evaluation results.</b></p> <p><b>The AM Plan shall reference the TOE component categorization report (DID F0016) for the certified version of the TOE.</b></p> <p><b>The AM Plan shall define the scope of changes to the TOE that are covered by the Plan.</b></p> <p><b>The AM Plan shall describe the TOE lifecycle, and shall identify the current plans for any new releases of the TOE, together with a brief description of any planned changes that are likely to have a significant security impact.</b></p> <p><b>The AM Plan shall describe the assurance maintenance cycle, stating and justifying the planned schedule of audits and target date of the next re-evaluation of the TOE.</b></p> <p><b>The AM Plan shall identify the individual(s) who will assume the role of developer security analyst for the TOE.</b></p> <p><b>The AM Plan shall describe how the developer security analyst role will ensure that the procedures documented or referenced in the AM Plan are followed.</b></p> <p>The AM Plan shall describe how the developer security analyst role will ensure that all developer actions involved in the analysis of the security impact of changes affecting the TOE are performed correctly.</p> <p>The AM Plan shall justify why the identified developer security analyst(s) have sufficient familiarity with the security target, function specification and (where appropriate) high-level design of the TOE, and with the evaluation results and all applicable assurance requirements for the certified version of the TOE.</p> <p>The AM Plan shall describe or reference the procedures to be applied to maintain the assurance in the TOE, which as a minimum shall include the procedures for configuration management, maintenance of assurance evidence, performance of the analysis of the security impact of changes affecting the TOE and flaw remediation.</p>	

DATA ITEM DESCRIPTION	
<b>1. TITLE</b> Component Categorization Report	<b>2. NUMBER</b> F016
<b>3. DESCRIPTION/PURPOSE</b> <p>The purpose of the Component Categorization Report I is to complement the Assurance Maintenance Plan (DID F015) by providing a categorization of the components of a TOE according to their relevance to security. This categorization acts as a focus for the developer's security impact analysis, and also for the subsequent re-evaluation of the TOE.</p>	
<b>4. DATA REQUIREMENTS</b> <p><b>Reference:</b> SOW paragraph 4.1.2, ISO/IEC 15408-3, AMA_CAT.1</p> <p><b>Contents:</b>  The TOE categorization report shall categorize each component of the TOE, identifiable in each TOE security function representation from the most abstract to the least abstract, according to its relevance to security; as a minimum, TOE components must be categorized as one of the TOE security policy enforcing or non TOE security policy enforcing.</p> <p>The TOE component categorization report shall describe the categorization scheme used, so that it can be determined how to categorize new components introduced into the TOE, and also when to re-categorize existing TOE components following changes to the TOE or its security target.</p> <p>The TOE component categorization report shall identify any tools used in the development environment that, it modified, will have an impact on the assurance that the TOE satisfies its security target.</p>	

DATA ITEM DESCRIPTION	
<b>1. TITLE</b> Evidence of Assurance Maintenance Documentation	<b>2. NUMBER</b> F017
<b>3. DESCRIPTION/PURPOSE</b> <p>The purpose of this documentation is to establish confidence that the assurance in the TOE is being maintained by the developer, in accordance with the AM Plan. This is achieved through the provision of evidence which demonstrates that the assurance in the TOE has been maintained which is independently checked by an evaluator. This check, termed an AM audit, is periodically applied during the lifetime of the Assurance Maintenance Plan (DID F015).</p>	
<b>4. DATA REQUIREMENTS</b> <p><b>Reference:</b> SOW paragraph 4.1.2, ISO/IEC 15408-3, AMA_EVD.1</p> <p><b><u>Contents:</u></b></p> <p>The assurance maintenance documentation shall include a configuration list and a list of identified vulnerabilities in the TOE.</p> <p>The configuration list shall describe the configuration items that comprise the current version of the TOE.</p> <p>The assurance maintenance documentation shall provide evidence that the procedures documented or referenced in the assurance maintenance plan are being followed.</p> <p>The list of identified vulnerabilities in the current version of the TOE shall show, for each vulnerability, that the vulnerability cannot be exploited in the intended environment for the TOE.</p>	

DATA ITEM DESCRIPTION	
<b>1. TITLE</b> Security Impact Analysis Documentation	<b>2. NUMBER</b> F018
<b>3. DESCRIPTION/PURPOSE</b>  The purpose of the Security Impact Analysis documentation is to provide confidence that assurance has been maintained in the TOE, through an analysis performed by the developer of the security impact of all changes affecting the TOE since it was certified.	
<b>4. DATA REQUIREMENTS</b>  <b>Reference:</b> SOW paragraph 4.1.2, ISO/IEC 15408-3, AMA_SIA.1  <b>Contents:</b> The security impact analysis shall identify all new and modified TOE components that are categorized as TOE security policy enforcing.  The security impact analysis shall, for each change affecting the security target or TOE security Function representations, briefly describe the change and any effects it has on lower representation levels.  The security impact analysis shall, for each change affecting the security target or TOE security function representations, identify all IT security functions and all TOE components categorized as TOE security policy enforcing that are affected by the change.  The security impact analysis shall, for each change which results in a modification of the implementation representation of the TOE security function or the IT environment, identify the test evidence that shows, to the required level of assurance, that the TOE security function continues to be correctly implemented following the change.  The security impact analysis shall, for each applicable assurance requirement in the configuration management (ACM), lifecycle support (ALC), delivery and operation (ADO), and guidance documents (AGD) assurance classes, identify any evaluation deliverables that have changed, and provide a brief description of each change and its impact on assurance.  The security impact analysis shall, for each applicable assurance requirement in the vulnerability assessment (AVA) assurance class, identify which evaluation deliverables have changed and which have not, and give reasons for the decision taken as to whether or not to update the deliverable.	

DATA ITEM DESCRIPTION	
<b>1. TITLE</b> Security Target	<b>2. NUMBER</b> F019
<b>3. DESCRIPTION/PURPOSE</b>  A Security Target (ST) represents a detailed design and architecture written in response to a Protection Profile. The IT security requirements chosen for a TOE and presented or cited in an ST need to be evaluated in order to confirm that they are internally consistent and lead to the development of a TOE that will meet its security objectives.	
<b>4. DATA REQUIREMENTS</b>  <b>Reference:</b> SOW paragraph 4.1.2, ISO/IEC 15408-1  <b>Contents:</b> 1.Security Target Introduction <b>The ST introduction shall contain an ST identification that provides the labeling and descriptive information necessary to control and identify the ST and the TOE to which it refers.</b>  <b>The ST introduction shall contain an ST overview that summarizes the ST in narrative form.</b>  <b>The ST introduction shall contain an ISO/IEC 15408 conformance claim that states any evaluatable claim of ISO/IEC 15408 conformance for the TOE.</b>  1.1 Security Target Identification 1.1.1 ST Name: 1.1.2 ST Identifier 1.1.3 Keywords 1.1.4 Evaluation Assurance Level (EAL) 1.1.5 ST Evaluation Status 1.2 Security Target Overview 1.2.1 ST Overview 1.2.2 Strength of Function 1.2.3 Related PPs, STs, and Referenced Documents 1.2.4 ST Organization 1.3 ISO/IEC 15408 Conformance  2 Description <b>The TOE description shall as a minimum describe the product or system type, and the scope and boundaries of the TOE in general terms both in a physical and logical way.</b>  2.1 System Type 2.2 System Assets 2.3 Security Enclaves  3 Security Environment <b>The statement of TOE security environment shall identify and explain any assumptions about the intended usage of the TOE and the environment of use of the TOE.</b>  <b>The statement of TOE security environment shall identify and explain any known or presumed threats to the assets against which protection will be required, either by the TOE or by its environment.</b>  <b>The statement of TOE security environment shall identify and explain any organizational security policies with which the TOE must comply.</b>	

### **3.1 Assumptions**

#### **3.1.1 Intended Use**

#### **3.1.2 Operational Environment**

#### **3.1.3 Connectivity**

### **3.2 Threats**

#### **3.2.1 Potential Threats to Assets by Security Enclave**

#### **3.2.2 Risk Mitigation Priority**

### **3.3 Organizational Security Policies**

#### **3.3.1 Accountability**

#### **3.3.2 Availability**

#### **3.3.3 Integrity**

#### **3.3.4 Confidentiality**

## **4. Security Objectives**

**The statement of security objectives shall define the security objectives for the TOE and its environment.**

**The security objectives for the TOE shall be clearly stated and traced back to aspects of the identified threats to be countered by the TOE and/or organizational security policies to be met by the TOE.**

**The security objectives for the environment shall be clearly stated and traced back to aspects of identified threats not completely countered by the TOE and/or organizational security policies or assumptions not completely met by all the TOE.**

#### **4.1 Security Objectives for the TOE**

#### **4.2 Security Objectives for the Operational Environment**

## **5. Security Requirements**

**The statement of TOE security functional requirements shall identify the TOE security functional requirements drawn from ISO/IEC 15408-2 functional requirements components.**

**The statement of TOE security assurance requirements shall identify the TOE security assurance requirements drawn from ISO/IEC 15408-3 assurance requirements components.**

**The statement of TOE security assurance requirements should include an Evaluation Assurance Level (EAL) as defined in ISO/IEC 15408-3.**

**The evidence shall justify that the statement of TOE security assurance requirements is appropriate.**

**The ST shall, if appropriate, identify any security requirements for the IT environment.**

**Operations on IT security requirements included in the ST shall be identified and performed.**

**Dependencies among IT security requirements included in the ST should be satisfied.**

**The evidence shall justify why any non-satisfaction of dependencies is appropriate.**

**The ST shall include a statement of the minimum strength of function level for the TOE security functional requirements, SOF-basic, SOF-medium, or SOF-high, as appropriate.**

**The ST shall identify any specific TOE security functional requirements for which an explicit strength of function is appropriate, together with the specific metric.**

## **5.1 Security Functional Requirements (SFRs)**

- 5.1.1 Level of Security Functionality and Security Integrity**
- 5.1.2 Security Training**
- 5.1.3 Integrity**
- 5.1.4 Availability**
- 5.1.5 Access Control**
- 5.1.6 Security Audit**
- 5.1.7 Confidentiality**
- 5.1.8 Identification and Authentication**
- 5.1.9 Recovery**
- 5.1.10 Security Management**

## **5.2 Security Assurance Requirements (SARs)**

- 5.2.1 Configuration Management (ACM)**
- 5.2.2 Delivery and Operation (ADO)**
- 5.2.3 Development (ADV)**
- 5.2.4 Guidance Documents (AGD)**
- 5.2.5 Lifecycle Support (ALC)**
- 5.2.6 Tests (ATE)**
- 5.2.7 Vulnerability Assessment (AVA)**
- 5.2.8 Maintenance of Assurance (AMA)**

## **5.3 Requirements for the IT Environment**

## **5.4 Requirements for the Non-IT Environment**

## **6 TOE Summary Specification (TSS)**

The TSS shall describe the IT security functions and the assurance measures of the TOE.

The TSS shall trace the IT security functions to the TOE security functional requirements such that it can be seen which IT security functions satisfy which TOE security functional requirements and that every IT security function contributes to the satisfaction of at least one TOE security functional requirement.

The IT security functions shall be defined in an informal style to a level of detail necessary for understanding their intent.

All references to security mechanisms included in the ST shall be traced to the relevant security functions so that it can be seen which security mechanisms are used in the implementation of each function.

The TSS shall trace the assurance measures to the assurance requirements so that it can be seen which measures contribute to the satisfaction of which requirements.

The TOE summary specification shall identify all IT security functions that are realized by a probabilistic or permutational mechanism, as appropriate.

The TSS shall, for each IT security function for which it is appropriate, state the strength of function claim either as a specific metric, or as SOF-basic, SOF-medium, or SOF-high.

## 6.1 TOE Security Functions

- 6.1.1 Level of Security Functionality and Security Integrity**
- 6.1.2 Security Training**
- 6.1.3 Integrity**
- 6.1.4 Availability**
- 6.1.5 Access Control**
- 6.1.6 Security Audit**
- 6.1.7 Confidentiality**
- 6.1.8 Identification and Authentication**
- 6.1.9 Recovery**
- 6.1.10 Security Management**

## 6.2 Assurance Measures

- 6.2.1 Configuration Management (ACM)**
- 6.2.2 Delivery and Operation (ADO)**
- 6.2.3 Development (ADV)**
- 6.2.4 Guidance Documents (AGD)**
- 6.2.5 Lifecycle Support (ALC)**
- 6.2.6 Tests (ATE)**
- 6.2.7 Vulnerability Assessment (AVA)**
- 6.2.8 Maintenance of Assurance (AMA)**

## 7 PP Claims

Each PP claim shall identify the PP for which compliance is being claimed, including qualifications needed for that claim.

Each PP claim shall identify the IT security requirements statements that satisfy the permitted operations of the PP or otherwise further qualify the PP requirements.

Each PP claim shall identify security objectives and IT security requirements statements contained in the SST that are in addition to those contained in the PP.

### 7.1 PP Reference

### 7.2 PP Tailoring

### 7.3 PP Additions

## **8 Rationale**

### **8.1 Security Objectives Rationale**

The security objectives rationale shall demonstrate that the stated security objectives are suitable to counter the identified threats to security.

The security objectives rationale shall demonstrate that the stated security objectives are suitable to cover all of the identified organizational security policies and assumptions.

### **8.2 Security Requirements Rationale**

The security requirements rationale shall demonstrate that the minimum strength of function level for the ST together with any explicit strength of function claim is consistent with the security objectives for the TOE.

The security requirements rationale shall demonstrate that the IT security requirements are suitable to meet the security objectives.

The security requirements rationale shall demonstrate that the set of IT security requirements together forms a mutually supportive and internally consistent whole.

### **8.3 TOE Summary Specification (TSS) Rationale**

The TSS rationale shall demonstrate that the IT security functions are suitable to meet the TOE security functional requirements.

The TSS rationale shall demonstrate that the combination of the specified IT security functions work together so as to satisfy the TOE security functional requirements.

The TSS rationale shall demonstrate that the assurance measures meet all assurance requirements of the TOE.

### **8.4 PP Claims Rationale**